HP 1:10Gb Ethernet BL-c Switch User Guide

Part Number 445876-001
May 2007 (First Edition)

Audience assumptions

This document is for the person who installs, administers, and troubleshoots servers and storage systems. HP assumes you are qualified in the servicing of computer equipment and trained in recognizing hazards in products with hazardous energy levels.

Contents

Introduction

In this section

Additional references

Configure the switch after installation. Detailed information about how to configure the switch is available in the reference guides listed below. To obtain these guides, see the HP website (http://www.hp.com/go/bladesystem/documentation).

- *HP 1:10Gb Ethernet BL-c Switch Application Guide*
- *HP 1:10Gb Ethernet BL-c Switch Command Reference Guide*
- *HP 1:10Gb Ethernet BL-c Switch Browser-based Interface Reference Guide*
- *HP 1:10Gb Ethernet BL-c Switch Quick Setup Instructions*

Features

The switch is designed for easy installation and high performance in an environment where traffic on the network and the number of users increases continually.

Enterprise class performance

The switch features include:

- Up to a 16-to-1 reduction in networking cables and connections, concentration of sixteen Gigabit Ethernet server ports down to as little as one Gigabit Ethernet port. This switch has the unique feature to provide both one Gigabit and ten Gigabit ports to the network, allowing the user the ultimate in network flexibility
- Fully supported on the HP c-Class BladeSystem server blade enclosure and infrastructure compatible with any combination of HP c-Class BladeSystem server blades
- Ability to replace an existing switch without having to power down the server blades or the server blade enclosure
- Pre-configured for immediate use with the HP c-Class BladeSystem server blade enclosure
- System security including SSH, SCP, 255 port-based IEEE 802.1Q tagged VLANs per switch, RADIUS user authentication and authorization, or TACACS+ AAA
- An extensive list of industry standard protocol support, compatible with widely-used networking components

- 9K jumbo frames that improve performance by increasing application throughput and decreasing server processor utilization
- Robust configuration and management from any switch port using the included browser-based and scriptable command line user interfaces.
- Support for Telnet, SNMP, SCP, FTP, and TFTP file transfer, human read/write configuration file, XModem, and an extensive list of MIB objects further enhance the management capabilities
- Fully redundant end-to-end architecture maximizing server availability from the network
- Support for IGMP snooping for multicasting
- Support for UFD for network path resiliency. It works in conjunction with NIC teaming functionality that is supported on the blade servers. This feature tracks the link state on uplink ports. When an uplink port goes down or is in STP blocking state, this feature will enable the switch to auto disable the downlinks which are connected to the blade server NICs. This enables NIC teaming software to detect link failure on the primary NIC port and fail over to the secondary NIC in the team. As a result, the secondary path is enabled for continued blade server access.

  When used in conjunction with UFD, NIC teams on the blade server must be configured for switch redundancy. That is, the team will span ports on both Switch 1 and Switch 2. See the *HP network adapter teaming: load balancing in ProLiant servers running Microsoft Windows operating systems* white paper for additional information. To locate this white paper:

  a. Go to the HP website (http://www.hp.com/support).
  b. Enter "nic" in the product search box.
  c. A product list displays. Select one of the NIC products.
  d. Select the "Manuals" link to display the documentation list. This white paper will be under the "White papers" category.
- RMON feature, which allows network devices to exchange network monitoring data. RMON performs these major functions:
  - Gathers cumulative statistics for Ethernet interfaces
  - Tracks a history of statistics for Ethernet interfaces
  - Creates and triggers alarms for user-defined events
- An administrator can define end user accounts that permit limited access to the switch. The switch requires username/password authentication for end users.
- Fast Uplink Convergence that enables the switch to quickly recover from the failure of the primary link or trunk group in a Layer 2 network using Spanning Tree Protocol.
- Support for SSH version 2. SSH is a protocol that enables remote administrators to log securely into the switch over a network to execute management commands.
- Switch software provides SNMP support for access through any network management software, such as HP OpenView.
- Support for HTTP software upgrade using the BBI. FTP or TFTP server is not required to perform a software upgrade.
- Port Fast Forwarding that allows a port that participates in Spanning Tree to bypass the Listening and Learning states and enter directly into the Forwarding state.
- Allows secure browser access (HTTPS) to management functions

Switch redundancy

In a dual switch configuration, the switches offer several redundancy and failover features. With these features, the network configuration is designed to allow for continued network access to each server blade in case of a component or link failure. The switch redundancy and failover features include:

- Up to eight separate switches per one HP c-Class BladeSystem server blade enclosure
- Up to four, one Gigabit Ethernet uplink ports and three, ten Gigabit Ethernet uplink ports (ports 19-21), per switch, for designing fully meshed uplink paths to the network backbone
- Server networking connections routed to each of the separate switches for redundant paths to tolerate a switch or port malfunction
- Redundant data path ten Gigabit Ethernet cross connection between switches
- STP support that eliminates potential problems caused by redundant networking paths and provides for failover with a secondary path in case of primary path failure; supports IEEE 802.1D Spanning Tree Protocol and is compatible with Cisco® PVST+ and Cisco PVST, when the other device is configured as untagged or configured to use 802.1q tagging. The switch also supports IEEE 802.1s MSTP and IEEE 802.1w RSTP.
- Redundant power supplies and redundant cooling fans within the server blade enclosure
- Redundant firmware images and configuration settings on switch flash memory
- Redundant, configurable DNS clients, syslog servers, gateways, and community strings and SNMP trap manager hosts

Configuration and management

The switch provides these configuration and management interfaces and tools:

- A scriptable CLI allows local, Telnet, or SSH access.
- An iSCLI that is software selectable.
- A BBI allows remote access using a Web browser such as Microsoft® Internet Explorer or Netscape Navigator.
- SNMP manageability and monitoring are supported.
- The switch functionality allows uploading and downloading of switch configurations through TFTP and SCP, thus allowing the rapid deployment of multiple server blade systems, and providing robust backup and restore capabilities.
- NTP is supported, allowing the switch to display and record the accurate date and time as provided by an NTP server.
- Two firmware images, either of which can be selected to be the current runtime image, can be held in memory.
- RADIUS provides support for user authentication and authorization.
- TACACS+ provides support for Cisco TACACS+ server compatible authentication, authorization, and accounting.
- The user interfaces provide multi-level password protected user accounts.
- IP settings are set manually or obtained automatically from a BOOTP server.

- A text-based, human read/write configuration file provides viewing, printing, and editing capabilities.
- A DNS client supports primary and secondary DNS servers.
- Any port can be enabled or disabled as desired.
- Any switch port can be used to perform switch management and PXE.

Diagnostic tools

The hardware, software, and firmware diagnostic tools that are available include:

- HP Systems Insight Manager automatic discovery and identification
- POST built into the switch boot process
- Switch port mirroring
- Switch LED panel displaying per port status and speed
- System, management, and option compatibility status LEDs
- Rear panel reset power switch and DB-9 management serial port
- Statistic monitoring including port utilization, data packets received/transmitted, port error packets, trunk utilization, and so on
- Ping and trace route capability
- Remote syslog with support for primary and secondary syslog server
- The ability to return the switch to known good condition in case of firmware corruption
- State information dump for tuning and debugging switch performance
- Panic command for immediate state dump to flash memory and automatic switch boot
- Ability to set NVRAM diagnostic flags

Switch architecture

The HP c-Class BladeSystem provides Ethernet switching technology for network cable reduction.

The switch does not affect or determine NIC enumeration and the associated mapping of NIC interfaces to switch ports. The numbering of the NICs on the server (for example, NIC 1, NIC 2, NIC 3) is determined by the server type, the server operating system, and what NICs are enabled on the server.

Port Mapping

For detailed port mapping information, see the HP BladeSystem enclosure installation poster or the HP BladeSystem enclosure setup and installation guide on the HP website (http://www.hp.com/go/bladesystem/documentation).

Dual switches

In a dual switch configuration, two switches in the server blade enclosure provide switch redundancy and redundant paths to the network ports on the server blades. Each switch has four, one Gigabit and three,

ten Gigabit external Ethernet ports and sixteen internal Gigabit Ethernet ports providing connectivity to the blade servers within the enclosure.

Redundant crosslinks

In a dual switch configuration, the two switches are connected through a single ten gigabit crosslink. This crosslink provides throughput of ten Gb/s for traffic between the switches.

This crosslink is disabled by default. This crosslink must be enabled for use.

Redundant paths to server bays

In a dual switch configuration, redundant Ethernet signals from each blade server are routed through the enclosure backplane to separate switches within the enclosure. This configuration provides redundant paths to each server bay.

Redundant Ethernet signals from each blade server are routed through the enclosure backplane to separate switches within the enclosure. However, specific switch port to server mapping varies depending on which type of server blade is installed.

On a heavily used system, using a single uplink port for 32 Ethernet signals causes a traffic bottleneck. For optimum performance, HP recommends using at least one uplink port per switch.

Supported technologies

Layer 2 switching

The switch uses Gigabit Layer 2 switching technology. Layer 2 refers to the Data Link layer of the OSI model, which is concerned with moving data packets across a network by enforcing CSMA/CD. This layer performs:

- Ethernet packet framing
- MAC addressing
- Physical medium transmission error detection
- Medium allocation (collision avoidance)
- Contention resolution (collision handling)

Layer 2 switching technology allows the switch to look into data packets and redirect them based on the destination MAC address. This reduces traffic congestion on the network because packets, instead of being transmitted to all ports, are transmitted to the destination port only.

Layer 3 switching

In addition to Layer 2 features, the switch also supports Layer 3 switching. Layer 3 switching features include:

- IP forwarding
- Static routing
- Dynamic routing based on RIP V1/V2 or OSPF protocols

- High availability VRRP

Layer 3 switching provides more power, flexibility, and security capabilities to network administrators. Network traffic is managed much more efficiently and broadcast traffic between servers remains within the enclosure. Security features provide added protection for switch configuration data, while packet filtering helps secure and segment sensitive traffic or network access.

IEEE 802.1 Q-based VLAN

The switch provides support for a total of 1000 IEEE 802.1Q VLANs for server grouping and isolation. A VLAN is a network segment configured according to a logical scheme rather than a physical layout. VLANs are used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN.

VLANs also logically segment the physical network into different broadcast domains so that packets are forwarded only between ports within the VLAN. This technology enhances performance by conserving bandwidth and improves security by limiting traffic to specific domains. For example, isolate the server blade iLO ports from the rest of the NICs. The iLO ports on Switch 2 are assigned to their own VLAN and go to a dedicated uplink or share an uplink using VLAN tagging.

IMPORTANT: The greater the number of VLANs, the greater the switch CPU utilization. For maximum switch performance, HP recommends being judicious when configuring the number of VLANs.

NOTE: VLAN 4095 is reserved for future functionality.

Spanning Tree Protocol

The switch supports IEEE 802.1D STP, which allows the blocking of links that form loops between switches in a network. When multiple links between switches are detected, a primary link is established. Duplicated links are blocked from use and become standby links. If the primary link fails, the standby link is activated.

In addition, the switch provides a spanning tree domain per VLAN. The switch is compatible with Cisco® PVST+ and Cisco PVST, when the other device is configured as untagged or configured to use 802.1q tagging. Thirty-two spanning tree domains are supported per switch.

NOTE: STP 32 is reserved for future functionality.

The switch also provides IEEE 802.1s-based MSTP and IEEE 802.1w-based RSTP.

SNMP

The switch is configured and monitored remotely from an SNMP-based network management station. The switch supports industry-standard SNMP MIBs and proprietary HP enterprise switch MIBs for fault detection and monitoring of switch functionality. In addition, the switch supports various environmental traps such as temperature and fan failure traps.

To secure the management interface, the switch administrator configures community strings with two levels of access: Read and Read/Write. Access to the switch is also restricted to only management stations that

are members of a specific IP network. This is achieved by configuring the address/mask of that specific network as a restricted management network address/mask.

Port mirroring

The switch allows mirroring of one or multiple ports (source ports) to another port (destination port) for network monitoring and troubleshooting purposes. This technology offers a way for network packet analyzers to view the traffic moving through the switch by providing a copy of the traffic that is currently being passed through any other port. The packets are sent to a network packet analyzer or other monitoring device attached to the mirror port.

Port trunking and load balancing

The switch supports EtherChannel compatible IEEE 802.3ad (without LACP) port trunking allowing several ports to be grouped together and act as a single logical link called a trunk. This feature provides a bandwidth that is a multiple of the bandwidth of a single link. It also improves reliability since load balancing is automatically applied to the ports in the trunked group. A link failure within the group causes the network traffic to be directed to the remaining links in the group.

TFTP support

TFTP support allows the switch firmware to be upgraded by downloading a new firmware file from a TFTP server to the switch. Firmware images of the switch are also uploaded to a TFTP server, a configuration file is downloaded into a switch from a TFTP server, and configuration settings are saved to the TFTP server.

Store and forward switching scheme

The switch provides a store and forward switching scheme that allows each packet to be buffered (stored) before it is forwarded to its destination. While this method creates latency, it improves reliability in a heavily used switch. Packets that cannot be forwarded are saved immediately, rather than dropped, so that packets behind them are less likely to be dropped in periods of heavy usage.

BOOTP

By default, the switch is configured to obtain an IP address from a BOOTP server during the boot process. The IP settings are also manually configured by means of the serial interface. The IP settings are configurable from the browser-based interface, but because the connection is based on an IP address for these interfaces, users will have to reconnect with the newly assigned IP address.

NTP

The switch maintains the current date and time. This information displays on the management interfaces and is used to record the date and time of switch events. Current date and time information are manually set on the switch or are obtained through NTP. NTP allows the switch to send a request to a primary NTP server in each polling period asking for GMT.

RADIUS

The switch supports the RADIUS method to authenticate and authorize remote administrators for managing the switch. This method is based on a client/server model. The RAS, the switch, is a client to the back-end database server. A remote user (the remote administrator) interacts only with the RAS, not the back-end server and database.

RADIUS authentication consists of:

- A protocol with a frame format that utilizes UDP over IP, based on RFC 2138 and 2866
- A centralized server that stores all the user authorization information
- A client, in this case, the switch

The switch, acting as the RADIUS client, communicates to the RADIUS server to authenticate and authorize a remote administrator using the protocol definitions specified in RFC 2138 and 2866. Transactions between the client and the RADIUS server are authenticated using a shared key that is not sent over the network. In addition, the remote administrator passwords are sent encrypted between the RADIUS client (the switch) and the back-end RADIUS server.

The benefits of using RADIUS are:

- Authentication of remote administrators
- Identification of the administrator using name/password
- Authorization of remote administrators
- Determination of the permitted actions and customizing service for individual administrators

TACACS+

The switch supports the TACACS+ method to authenticate, authorize, and account for remote administrators managing the switch. This method is based on a client/server model. The switch is a client to the back-end TACACS+ AAA server. A remote user (the remote administrator) interacts only with the client, and not with the back end AAA server.

The TACACS+ AAA method consists of:

- A protocol with a frame format that utilizes TCP over IP
- A centralized AAA server that stores all the user authentication, authorization, and accounting (of usage) information
- A NAS or client (in this case, the switch)

The switch, acting as the TACACS+ client or NAS, communicates to the TACACS+ server to authenticate, authorize, and account for user access. Transactions between the client and the TACACS+ server are authenticated using a shared key that is not sent over the network. In addition, the remote administrator passwords are sent encrypted between the TACACS+ client (the switch) and the back-end TACACS+ server.

The switch supports:

- Only standard ASCII inbound login authentication. PAP, CHAP, or ARAP login methods are not supported. One-time password authentication is also not supported.
- Authorization privilege levels of only 0, 3, and 6. These map to management levels of user, oper, and admin, respectively.

- The accounting attributes of protocol, start_time, stop_time, and elapsed_time. For BBI users, accounting stop records are only sent if the user presses the QUIT button.

SSH and SCP

SSH and SCP use secure tunnels to encrypt and secure messages between a remote administrator and the switch. Telnet does not provide this level of security. The Telnet method of managing a switch does not provide a secure connection.

SSH is a protocol that enables remote administrators to log securely into the switch over a network to execute management commands.

SCP is used to copy files securely from one machine to another. SCP uses SSH for encryption of data on the network. On a switch, SCP is used to download and upload the switch configuration via secure channels.

XModem

The switch supports XModem for transferring files during direct dial-up communications. XModem sends blocks of data in 128-byte blocks, and includes an error-detection system called a checksum. When the data is received, the error detection system ensures that the entire message reached its destination. If not, the receiving computer sends a request for retransmission of the data.

IGMP Snooping

The switch supports IGMP Snooping for multicasting. Version 1-, Version 2-, and Version 3-based IGMP Snooping are supported. In addition, auto detection of the multicast router port and manual configuration of the multicast router port is supported. For efficient multicast traffic management, the IGMP Filtering option is supported.

Jumbo frames

By default, the switch supports jumbo frames up to 9216 bytes, which help reduce server CPU utilization and increase application throughput. No configuration is required. The switch does not fragment frames as they exit, or assemble packets into jumbo frames as they enter the switch.

Auto-MDI/MDIX

The switch RJ-45 Ethernet ports are MDI/MDI crossover capable. MDI/MDIX is a type of Ethernet port connection using twisted pair cabling. The MDI is the component of the MAU that provides the physical and electrical connection to the cabling medium. An MDIX is a version of MDI that enables connection between like devices. MDI ports connect to MDIX ports via straight-through twisted pair cabling whereas both MDI-to-MDI and MDIX-to-MDIX connections use crossover twisted pair cabling. The switch has the capability to automatically detect the cable selection/type, making the distinction between a straight-through cable and a crossover cable unimportant.

Auto-negotiation of duplex mode and speed on 1 Gigabit ports

Auto-negotiation of duplex mode and speed are configured on the switch. Network adapters that support multiple data speeds, such as Fast Ethernet and Gigabit Ethernet, choose the speed at which they run

through a procedure called auto-negotiation. Auto-negotiation involves probing the capability of the network using low-level signaling techniques to select compatible Ethernet speeds. Auto-negotiation was originally developed to make the migration from traditional Ethernet to Fast Ethernet products easier.

Redundant images in firmware

The switch stores up to two different software images, called image1 and image2, as well as boot software, called boot. When downloading new software, the ability to specify where it is to be placed (into image1, image2, or boot) is activated.

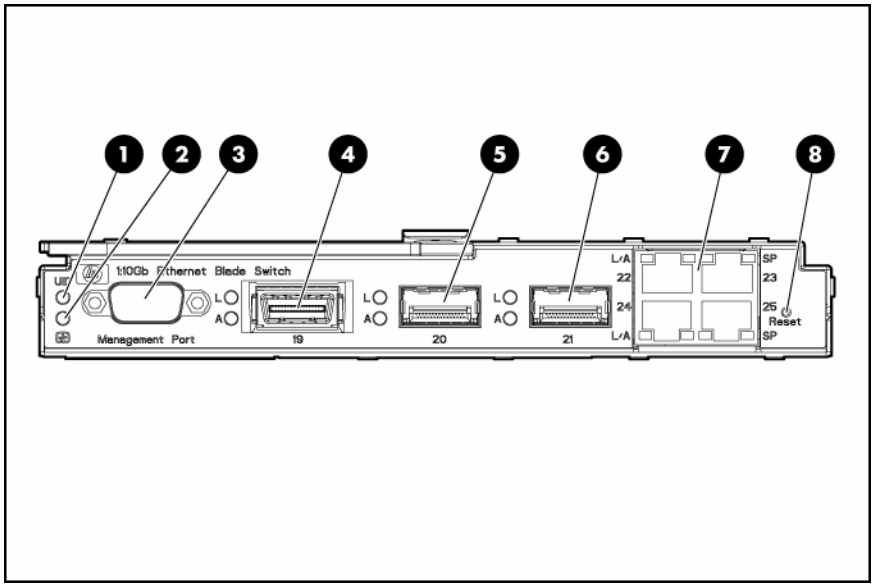
For example, if the active image is currently loaded into image1, load the new image software into image2. This allows a test of the new software and the option to revert back to the original image stored in image1, if needed.

△ **CAUTION:** Unlike the firmware that has two images, there is only one image of boot supported. Upgrading the boot image replaces the original boot image.

Component identification

In this section

1:10Gb Ethernet Blade Switch front panel



CAUTION: Pressing the Reset button while the Health LED is green resets the switch.

Item	Description
1	UID LED
2	Health LED • Off—Not powered up • Green—Powered up and all ports match • Amber—Indicates a problem such as a port mismatch. For more information, see the HP BladeSystem enclosure setup and installation guide.
3	DB-9 management serial port
4	CX4 connector port 19 • Link LED (top)—Green • Activity LED (bottom)—Flashing green
5	XFP transceiver cage port 20 • Link LED (top)—Green • Activity LED (bottom)—Flashing green

Item	Description
6	XFP transceiver cage port 21 • Green—Link LED (top) • Flashing green—Activity LED (bottom)
7	RJ-45 ports 22-25 Speed LED (right) • Off—10 Mb/s • Green—100 Mb/s • Amber—1 Gb/s Activity/Link LED (left) • Green—Link • Flashing green—Activity
8	Reset button

Installing the switch

In this section

Preparing for installation

IMPORTANT: Before installing the switch, make a record of the MAC address (printed on the MAC address label attached to the switch). This address is needed when configuring the switch.

Planning the switch configuration

The switch ships with a default configuration in which all downlink and uplink ports are enabled and assigned a default VLAN with a VID equal to 1. This default configuration simplifies the initial setup by allowing use of a single uplink cable (from any external Ethernet connector) to connect the server blade enclosure to the network. Assess the particular server environment to determine any requirements for other considerations.

The switch does not affect or determine NIC numeration and the associated mapping of NIC interfaces to switch ports. The numbering of the NICs on the server (for example, NIC 1, NIC 2, NIC 3) is determined by the server type, the server operating system, and which NICs are enabled on the server.

NOTE: Port 18 is reserved for connection to the Onboard Administrator module for switch management. This allows a user to enable the functionality of future firmware upgrade releases.

The Onboard Administrator module controls all port enabling. Enabling is based on matching ports between the server and the interconnect bay. Before power up, the Onboard Administrator module verifies that the server NIC option matches the switch bay that is selected and enables all ports for the NICs installed.

For detailed port mapping information, see the HP BladeSystem enclosure installation poster or the HP BladeSystem enclosure setup and installation guide on the HP website (http://www.hp.com/go/bladesystem/documentation).

Default settings

When planning the configuration, consider the default settings for these parameters:

- Switch IP settings
- VLAN settings
- XFP settings
- Port names and types
- Port trunking settings
- Interswitch X-Connect port settings
- SNMP settings
- User name and password settings
- Default access to various management interfaces
- NTP settings

IMPORTANT: See "Runtime switching software default settings (on page 33)" for a complete list of default configuration settings.

Switch security

When planning the switch configuration, secure access to the management interface by:

- Creating users with various access levels
- Enabling or disabling access to various management interfaces to fit the security policy
- Changing default SNMP community strings for read-only and read-write access

User, operator, and administrator access rights

To enable better switch management and user accountability, three levels or classes of user access have been implemented on the switch. Levels of access to CLI, Web management functions, and screens increase as needed to perform various switch management tasks. Conceptually, access classes are defined as:

- User interaction with the switch is completely passive. Nothing can be changed on the switch. Users can display information that has no security or privacy implications, such as switch statistics and current operational state information.
- Operators can only effect temporary changes on the switch. These changes will be lost when the switch is rebooted/reset. Operators have access to the switch management features used for daily switch operations. Because any changes an operator makes are undone by a reset of the switch, operators cannot severely impact switch operation.
- Administrators are the only ones that can make permanent changes to the switch configuration, changes that are persistent across a reboot/reset of the switch. Administrators can access switch functions to configure and troubleshoot problems on the switch. Because administrators can also make temporary (operator-level) changes as well, they must be aware of the interactions between temporary and permanent changes.

Access to switch functions is controlled through the use of unique user names and passwords. Once connected to the switch via the local console, Telnet, or SSH, a password prompt appears.

NOTE: It is recommended to change the default switch passwords after initial configuration and as regularly as required under the network security policies. For more information, see the *HP 1:10Gb Ethernet BL-c Switch Command Reference Guide*.

The default user name and password for each access level are:

User account	Description and tasks performed	Password
User	The user has no direct responsibility for switch management. He or she can view all switch status information and statistics, but cannot make any configuration changes to the switch.	user
Operator	The operator manages all functions of the switch. The operator can reset ports or the entire switch. By default, the operator account is disabled and has no password.	
Administrator	The super user administrator has complete access to all menus, information, and configuration commands on the switch, including the ability to change both the user and administrator passwords.	admin

Manually configuring a switch

The switch is configured manually using a command line interface, a browser-based interface, or an SNMP interface. See the *HP 1:10Gb Ethernet BL-c Switch Command Reference Guide* for more information on using these management interfaces to configure the switch.

After a switch is configured, back up the configuration as a text file to a TFTP server. The backup configuration file is then downloaded from the TFTP server to restore the switch back to the original configuration. This restoration is necessary if one of these conditions apply:

- The switch configuration becomes corrupted during operation.
- The switch must be replaced because of a hardware failure.

Configuring multiple switches

Configure multiple switches by using scripted CLI commands through Telnet or by downloading a configuration file using a TFTP server.

Using scripted CLI commands through Telnet

The CLI, provided with the switch, executes customized configuration scripts on multiple switches. A configuration script is tailored to one of the multiple switches, and then that configuration can be deployed to other switches from a central deployment server.

Using a configuration file

If planning for the base configuration of multiple switches in a network to be the same, manually configure one switch, upload the configuration to a TFTP server, and use that configuration as a base configuration template file.

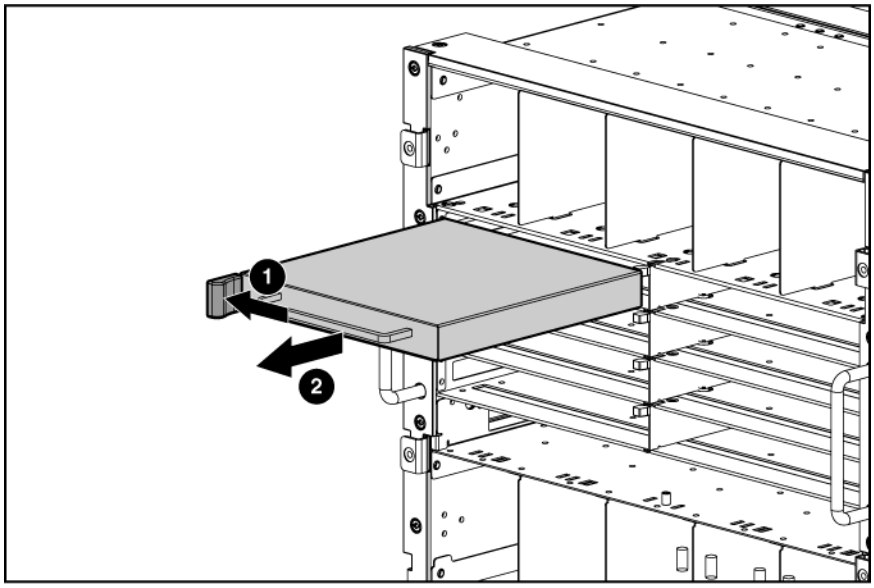
Switch IP addresses are acquired by default using BOOTP, therefore, each switch has a unique IP address. Each switch is remotely accessed from a central deployment server and an individual switch configuration is downloaded to meet specific network requirements. See the *HP 1:10Gb Ethernet BL-c Switch Command Reference Guide* for additional information on using a TFTP server to upload and download configuration files.

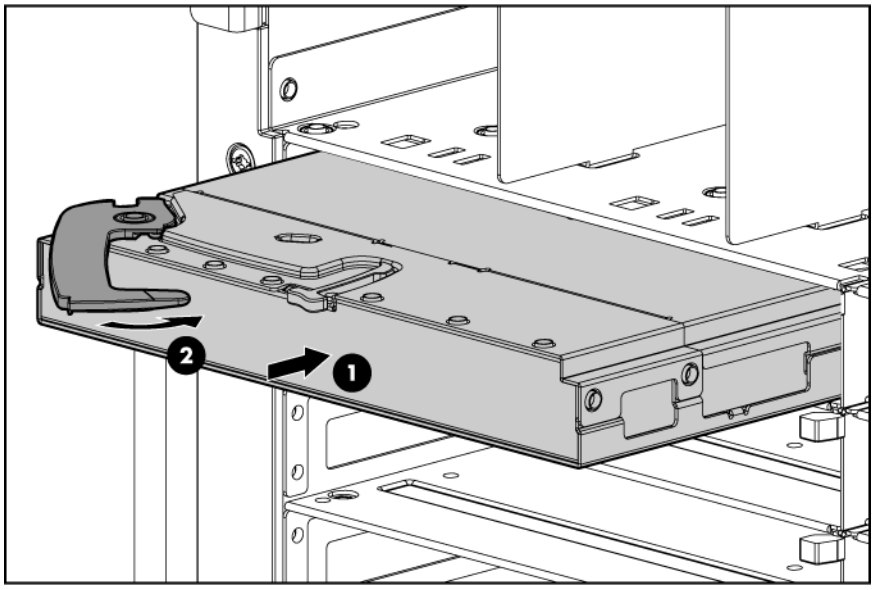
Installing the switch

CAUTION: Do not cable the switch until after configuration.

IMPORTANT: Make sure that the server NIC configuration matches the switch bay selected.

NOTE: When installing two switches, there is one switch interconnect port between adjacent I/O bays. Port 17 is disabled by default. The port must be manually enabled to use.





A successful installation is indicated by a green Health LED. If the Health LED is amber or power is not applied to the switch, see the "Troubleshooting" section of the HP BladeSystem enclosure setup and installation guide for more information.

Accessing the switch

The switch is accessed remotely using the Ethernet ports or locally using the DB-9 management serial port.

To access the switch remotely:

1. Assign an IP address. By default, the switch is set up to obtain its IP address from a BOOTP server existing on the attached network.
2. From the BOOTP server, use the switch MAC address to obtain the switch IP address.
3. From a computer connected to the same network, use the IP address to access the switch using a Web browser or telnet application, which enables access to the switch BBI or CLI. The switch logon prompt appears.

NOTE: If the switch does not obtain the IP address by means of the BOOTP service, access the switch locally and configure the IP address manually. After assigning the IP address to the switch, then access the switch remotely.

To access the switch locally:

1. Connect the switch DB-9 serial connector, using a null-modem serial cable to a local client device (such as a laptop computer) with VT100 terminal emulation software.
2. Open a VT100 terminal emulation session with these settings: 9600 baud rate, eight data bits, no parity, one stop bit, and no flow control.

Logging on and configuring the switch

To log on to the switch:

1. Access the switch ("Accessing the switch" on page 22). After connecting to the switch console, the login prompt appears.

```
Enter password:
```

2. Enter `admin` as the default administrator password.

   The Main Menu appears and displays all administrator privileges:

```
[Main Menu]
   info       - Information Menu
   stats      - Statistics Menu
   cfg        - Configuration Menu
   oper       - Operations Command Menu
   boot       - Boot Options Menu
   maint      - Maintenance Menu
   diff       - Show pending config changes  [global command]
   apply      - Apply pending config changes [global command]
   save       - Save updated config to FLASH [global command]
   revert     - Revert pending or applied changes [global command]
   exit       - Exit  [global command, always available]

>> Main#
```

See the *HP 1:10Gb Ethernet Blade Switch for c-Class BladeSystem Command Reference Guide* for information on configuring the IP address, changing configuration settings, and monitoring switch operation using one of the following interfaces:

- Local RS-232 serial console management interface
- Remote telnet console management interface

See the *HP 1:10Gb Ethernet Blade Switch for c-Class BladeSystem Browser-based Interface Reference Guide* for information on using the embedded HTML interface to manage the switch from anywhere on the network using a standard browser, such as Netscape Navigator or Microsoft® Internet Explorer.

See "SNMP MIBs support (on page 48)" for more information on the SNMP agents. This section also describes how to use the MIBs to configure and monitor the switch using a generic SNMP manager, such as HP OpenView Network Node Manager or HP Systems Insight Manager.

Installing XFP transceivers

CAUTION: To prevent damage to the fiber optic cable or the XFP transceiver, do not install or remove fiber-optic XFP transceivers with cables attached. Disconnect all cables from the XFP transceiver before removing or installing an XFP transceiver.

CAUTION: Removing and installing an XFP transceiver can shorten the useful life. Do not remove and insert XFP transceivers more often than is necessary.

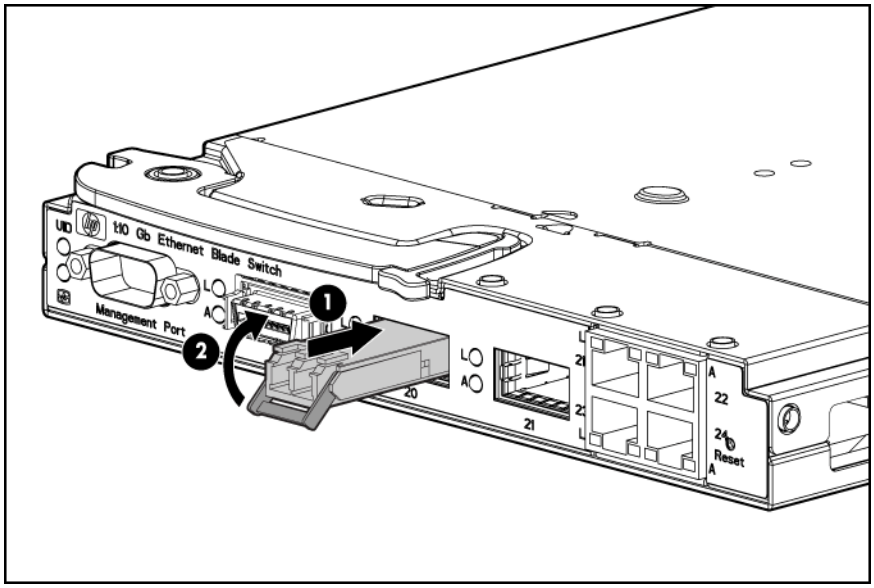
CAUTION: HP recommends attaching an ESD-preventative wrist strap to your wrist and to a bare metal surface on the chassis to prevent electrostatic discharge.

CAUTION: Do not remove the dust plugs from the fiber-optic XFP transceiver or the rubber caps from the fiber-optic cable until you are ready to connect the cable. The plugs and caps protect the XFP transceiver ports and cables from contamination and ambient light.

1. Remove the dust plug and save for future use.

IMPORTANT: Use only XFP transceivers purchased from HP.

2. Insert the XFP transceiver. With latch closed, be sure that the transceiver is fully seated and securely in place.



Supporting software and special considerations

Supporting software is available to assist in configuring and managing the switch.

- Server Blade and Power Management Module Firmware—Provides firmware and installation instructions required for proper rack location operation.
- Utilities package and documentation—Provides utilities and documentation for switch management.

- Firmware Upgrade Smart Component (for Microsoft Windows only)—Provides quick and easy installation of the switch firmware, firmware upgrade tool, and `readme` file. A SoftPaq is available for use with Linux operating systems.

The utilities package and documentation, and the SoftPaq listed above, are available on the HP website (http://www.hp.com/go/bladesystem/documentation).

Replacing a switch

In this section

Replacing an existing switch

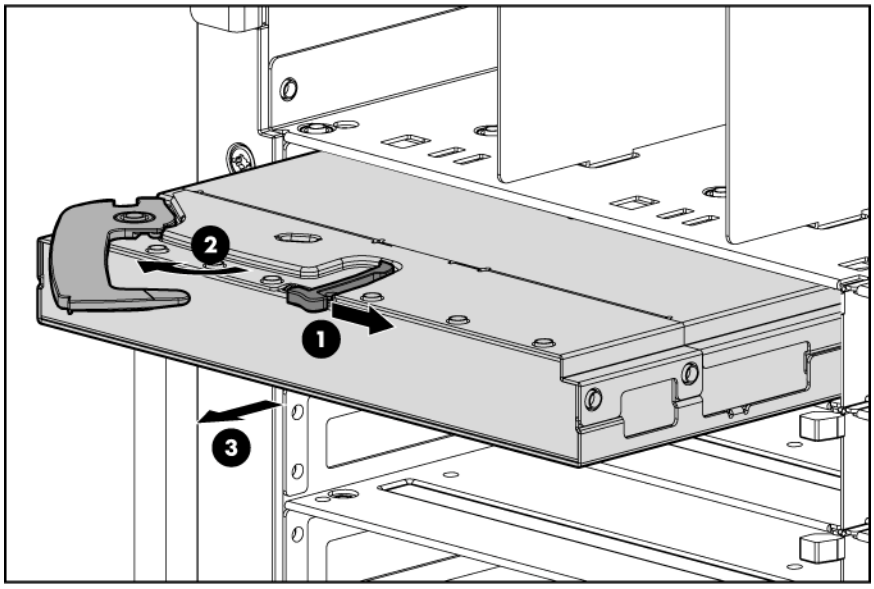
CAUTION: Removing the switch from a powered enclosure results in the loss of network communications between the server blade network ports that are connected through this switch and the segment of network infrastructure those ports need to communicate.

For continued blade server network communication and services availability before removing the switch, redirect critical high-availability services or applications to use the redundant network ports available on those blade servers that are connected through the redundant switch in the enclosure.

CAUTION: Do not cable the switch until after configuration.

To replace an existing switch:

1. Save the configuration file to a TFTP server for later retrieval. For more information on saving a configuration file to a TFTP server, see the *HP 1:10Gb Ethernet BL-c Switch Command Reference Guide*.
2. Remove and label the cables.
3. Remove the switch.



4. Slide the new switch fully into the interconnect bay. For more installation information, see "Installing the switch (on page 21)."

5. Close the ejector lever and wait for the switch boot up completely.
6. If the configuration file was saved to a TFTP server, download the configuration. For more information on downloading a configuration file, see the *HP 1:10Gb Ethernet BL-c Switch Command Reference Guide*.

Regulatory compliance notices

In this section

Class A equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at personal expense.

Modifications

The FCC requires the user to be notified that any changes or modifications made to this device that are not expressly approved by Hewlett-Packard Company may void the user's authority to operate the equipment.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Canadian notice

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe A respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

European Union regulatory notice

This product complies with the following EU Directives:

- Low Voltage Directive 2006/95/EC
- EMC Directive 2004/108/EC

Compliance with these directives implies conformity to applicable harmonized European standards (European Norms) which are listed on the EU Declaration of Conformity issued by Hewlett-Packard for this product or product family.

This compliance is indicated by the following conformity marking placed on the product:

CE

This marking is valid for non-Telecom products and EU harmonized Telecom products (e.g. Bluetooth).

CE(xxxx*)①

This marking is valid for EU non-harmonized Telecom products.

*Notified body number (used only if applicable—refer to the product label)

Hewlett-Packard GmbH, HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, Germany

BSMI notice

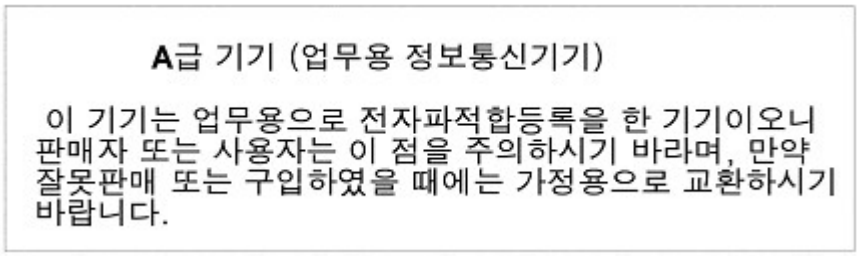
警告使用者:

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Japanese class A notice

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Korean class A notice



Laser compliance

This product may be provided with an optical storage device (that is, CD or DVD drive) and/or fiber optic transceiver. Each of these devices contains a laser that is classified as a Class 1 Laser Product in accordance with US FDA regulations and the IEC 60825-1. The product does not emit hazardous laser radiation.

Each laser product complies with 21 CFR 1040.10 and 1040.11 except for deviations pursuant to Laser Notice No. 50, dated May 27, 2001; and with IEC 60825-1:1993/A2:2001.

⚠ **WARNING:** Use of controls or adjustments or performance of procedures other than those specified herein or in the laser product's installation guide may result in hazardous radiation exposure. To reduce the risk of exposure to hazardous radiation:

- Do not try to open the module enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP Authorized Service technicians to repair the unit.

The Center for Devices and Radiological Health (CDRH) of the U.S. Food and Drug Administration implemented regulations for laser products on August 2, 1976. These regulations apply to laser products manufactured from August 1, 1976. Compliance is mandatory for products marketed in the United States.

Technical specifications

In this section

General specifications

Category	Specification
Standards:	IEEE 802.3 10Base-T Ethernet IEEE 802.3u 100Base-TX Fast Ethernet IEEE 802.3ab 1000Base-T Ethernet IEEE 802.3z 1000Base-SX Ethernet IEEE 802.1D Spanning Tree Protocol IEEE 802.1s Multiple Spanning Tree Protocol IEEE 802.1w Rapid Spanning Tree Protocol IEEE 802.1Q VLAN IEEE 802.3ac Frame Extensions for VLAN IEEE 802.3ad Link Aggregation Protocol (No LACP support) IEEE 802.3x Full-Duplex Flow Control ANSI/IEEE 802.3 Nway Auto-Negotiation
Protocols:	CSMA/CD
Data transfer rates:	
Ethernet	Half-Duplex: 10 Mb/s Full-Duplex: 20 Mb/s
Fast Ethernet	Half-Duplex: 100 Mb/s Full-Duplex: 200 Mb/s
Gigabit Ethernet	Half-Duplex: 1000 Mb/s Full-Duplex: 2000 Mb/s
10Gb Ethernet	Half-Duplex: 10000 Mb/s Full-Duplex: 20000 Mb/s
Connectors:	
HP 1:10Gb Ethernet BL-c Switch	4 RJ-45, 1 DB-9, 2 10 Gb XFP, 1 10 Gb CX4
10Base-T	Two Pair UTP Category 3, 4, 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)

Category	Specification
100Base-TX	Two Pair or Four Pair UTP Category 5 (100 m) EIA/TIA-568 100-ohm STP (100 m)
1000Base-T	Four Pair UTP Category 5e (100 m) EIA/TIA-568 100-ohm STP (100 m)
10 Gb multimode fiber cable	62.5/125 or 50/125 microns
10 Gb singlemode fiber cable	9/25 micron
10 Gb CX4 copper cable	Use only these approved HP cables: • HP BLadeSystem c-Class .5m 10-GbE CX4 cable (PN 444477-B21) • HP BLadeSystem c-Class 1m 10-GbE CX4 cable (PN 444477-B22) • HP BLadeSystem c-Class 15m 10-GbE CX4 cable (PN 444477-B27)
Number of ports per switch:	16 x 1000-Mb/s ports dedicated to the server blade for switch communications 1 x 10 Gb/s ports dedicated to communications between switches that are inserted in ports 1 and 2, 3 and 4, 5 and 6 or 7 and 8 4 x 10Base-T/100Base-TX/1000Base-T RJ-45 ports 1 x serial RS-232 DB-9 rear panel management serial port 2 x XFP 10 Gb SR/LR transceivers 1 x CX4 10 Gb/s

Port names, VLANs, STP, trunking default settings

These default settings apply to all ports:

- Speed—Autonegotiate

  Port 18: speed—100, auto—off

  Port 19: speed—10000, auto—off

  Port 20: speed—10000, auto—off

  Port 21: speed—10000, auto—off

  Port 22: speed—auto

  Port 23: speed—auto

  Port 24: speed—auto

  Port 25: speed—auto
- PVID—1
- Tag (Y/N)—N
- VLAN Name—Default VLAN

Port type	Port number	Port name	STP
Server	1	Downlink1	Disabled
Server	2	Downlink2	Disabled
Server	3	Downlink3	Disabled

Port type	Port number	Port name	STP
Server	4	Downlink4	Disabled
Server	5	Downlink5	Disabled
Server	6	Downlink6	Disabled
Server	7	Downlink7	Disabled
Server	8	Downlink8	Disabled
Server	9	Downlink9	Disabled
Server	10	Downlink10	Disabled
Server	11	Downlink11	Disabled
Server	12	Downlink12	Disabled
Server	13	Downlink13	Disabled
Server	14	Downlink14	Disabled
Server	15	Downlink15	Disabled
Server	16	Downlink16	Disabled
X-Connect	17	XConnect1	Enabled
Mgmt	18	Mgmt	Enabled
Uplink	19	Uplink1	Enabled
Uplink	20	Uplink2	Enabled
Uplink	21	Uplink3	Enabled
Uplink	22	Uplink4	Enabled
Uplink	23	Uplink5	Enabled
Uplink	24	Uplink6	Enabled
Uplink	25	Uplink7	Enabled

Runtime switching software default settings

General default settings

Setting	Value
Notice	None
Banner	None
User names and passwords	User names and passwords: • user—Enabled, password is `user` • oper—Disabled, no password • admin—Enabled (cannot be disabled), password is `admin`
BOOTP service	Enabled
IP address (if manual IP option is selected)	0.0.0.0
Subnet mask (if manual IP option is selected)	0.0.0.0

Setting	Value
Primary default gateway	0.0.0.0
Secondary default gateway	0.0.0.0
Primary DNS server address	0.0.0.0
Secondary DNS server address	0.0.0.0
Default domain name	None
Management network/mask	0.0.0.0 / 0.0.0.0
Switch software image on next boot	Image 1
Switch Config file on next boot	Active
Display Hostname (sysName) in CLI prompt	Disabled
Idle timeout	5 minutes
Telnet status	Enabled
Telnet port	23
Web status	Enabled
Web port	80
Backpressure	Disabled
Port state	Enabled
Port speed/duplex	Auto
Flow control	Receive & transmit
STP	STG 1—Enabled with default VLAN (VID=1) Port 1-16 (server ports) STP—Disabled at port level STG 2-16—Disabled
Bridge Max Age	20 seconds
Bridge Hello Time	2 seconds
Bridge Forward Delay	15 seconds
Bridge Priority	32768
MAC Address Aging Time	300 seconds
Port Priority	128
Path Cost	4
Static VLAN Entry	Default VLAN (VID = 1)
Port VID	1 for all ports
Port Trunking	Trunk group 1, enabled with port 17 and 18

Setting	Value
Port Trunking Load Sharing Algorithm	The algorithm selects the following as forwarding ports for forwarding traffic: 1 For forwarding IP Packets—modulus of XOR of last 3 bits of source and last 3 bits of Destination IP address 2 For forwarding non-IP packets—modulus of XOR of last 3 bits of source and last 3 bits of Destination MAC address 3 For forwarding broadcast, multicast packets, and unknown unicast packets—the lowest active port number in the trunk group
Port Mirroring-Mirror Status	Disabled
Port Mirroring-Mirror Port	None selected
Port Mirroring-Mirror Port Traffic Direction	None selected
Port Mirroring-Monitoring Port	None selected
SNMP	Read/write
SNMP System Name	None
SNMP System Location	None
SNMP System Contact	None
SNMP Community String/Access Right	Public—read-only Private—read/write
SNMP Trap Host 1	0.0.0.0
SNMP Trap Host 1 Community String	Public
SNMP Trap Host 2	0.0.0.0
SNMP Trap Host 2 Community String	Public
SNMP Authentication Traps	Disabled
SNMP Link Up/Down Traps	Enabled
Security IP Network/Mask	0.0.0.0 / 0.0.0.0
TFTP Server IP Address	0.0.0.0
TFTP Port Number	69
Firmware upgrade	File name—none
Configuration file from TFTP server	File name—none
Configuration file to TFTP server	File name—none
PING tool	Target address—undefined Default tries—5
Trace Route tools	Target address—undefined
Serial Port Baud Rate	9600
Serial Port Data Bit	8

Setting	Value
Serial Port Parity Bit	None
Serial Port Stop Bit	1
Serial Port Flow Control	None
Default VLAN	Default VLAN (VID=1) with all ports assigned including CPU, STG=1
NTP State	Disabled
NTP Server	0.0.0.0
NTP Resync Interval	720 minutes
GMT Timezone Offset	-06:00
Daylight Savings Time State	Disabled
System Up Time	0 days 00 :00 :00
Current time	RTC or NTP (00 :00 :00)
Date	None
Syslog Host	0.0.0.0
Syslog Host 2	0.0.0.0
Syslog Host Severity	7
Syslog Host 2 Severity	7
Syslog Console Output	Disabled
Log	• console—Enabled • system—Enabled • mgmt—Enabled • cli—Enabled • stp—Enabled • vlan—Enabled • ssh—Enabled • ntp—Enabled • ip—Enabled • web—Enabled
RSA Server Key Autogen Interval	0
RSA Server Key Autogen	Disabled
SSH Server	On
SCP-only Administrator Password	admin
SSH Server Port	22
SCP Apply and Save	Disabled
RADIUS Server	Off
RADIUS Secret	None
Primary RADIUS Server	0.0.0.0
Secondary RADIUS Server	0.0.0.0

Setting	Value
RADIUS Server Port	1645
RADIUS Server Retries	3
RADIUS Server Timeout	3
RADIUS Backdoor for Telnet Access	Disabled
Re-ARP Period in Minutes	10
MSTP	Disabled
MSTP Default Mode	RSTP
MSTP Region Name	None
MSTP Region Version	1
MSTP Max Hop Count	20
CIST Bridge Max Age	20 seconds
CIST Bridge Hello Time	2 seconds
CIST Bridge Forward Delay	15 seconds
CIST Bridge Priority	32768
CIST MAC Address Aging Time	300 seconds
CIST Port Priority	128
CIST Port Path Cost	20000
MSTP Link Type	Auto
MSTP Edge Port	Enabled: ports 1-16
TACACS+ Service	Off
TACACS+ Primary Secret	None
TACACS+ Secondary Secret	None
Primary TACACS+ Server	0.0.0.0
Secondary TACACS+ Server	0.0.0.0
TACACS+ Server Port	49
TACACS+ Server Retries	3
TACACS+ Server Timeout	5 seconds
TACACS+ Backdoor for Telnet Access	Disabled
IGMP Snooping	Disabled
IGMP VLANs	None
IGMP Report Timeout	10 seconds
IGMP Multicast Router Timeout	255 seconds
IGMP Robust	2

Setting	Value
Aggregate IGMP Report	Disabled
IGMP Fastleave	Disabled
IGMP Fastleave VLANs	None
IGMP Filtering	Disabled
IGMP Filters	None
Static Multicast Router Port	None
Uplink Failure Detection (UFD)	Off
UFD Failure Detection Pair	Disabled
UFD Link To Monitor - Port	None
UFD Link To Monitor - Trunk	None
UFD Link to Disable - Ports	None
UFD Link To Disable - Trunks	None
RMON History Group Number	None
RMON History Interface MIB to Monitor	None
RMON History Number of Requested Buckets	30
RMON History Polling Interval	1800
RMON History Owner	None
RMON Event Group Number	None
RMON Event Description	None
RMON Event Type	None
RMON Alarm Group Number	None
RMON Alarm MIB to Monitor	None
RMON Alarm Interval	1800
RMON Alarm Sample Type	abs
RMON Alarm Type	either
RMON Alarm Rising Threshold	0
RMON Alarm Falling Threshold	0
RMON Alarm Rising Event Index	0

Setting	Value
RMON Alarm Falling Event Index	0
RMON Alarm Owner	Null
IP Forwarding	Disabled
Configurable User Name - admpw	admin
Configurable User Name - opw	Disabled
Configurable User Name - usrpw	user
Configurable User Name - UID 1-10	Disabled
Uplink Fast	Disabled
THASH - enable	SIP and DIP
SNMPv1 - Read community string:	public
SNMPv1 - Write community string:	private
SNMPv1 - SNMP state machine timeout:	5
SNMPv1 - authentication traps:	Disabled
SNMPv1 - Uplink Failure Detection traps:	Disabled
SNMPv1 - link up/down traps:	Enabled
SNMPv1 - v1/v2 access:	Enabled
IGMP	off
MCAST/BCAST/UCAST	off
SNMPv3 - SNMP access	read/write enabled
SNMPv3 - v1v2 access	Enabled
SNMPv3 - adminmd5	authentication = md5, privacy = des
SNMPv3 - adminsha	authentication = sha, privacy = des
SNMPv3 - v1v2only	authentication = none, privacy = none
SNMPv3 - admingrp	level=authPriv, users=adminmd5, adminsha, rview, wview, nview=iso
SNMPv3 - v1v2grp	level=noAuthNoPriv, users=v1v2only, rview, wview=iso, nview=v1v2only
SNMPv3 - iso	subtree = 1, included

Setting	Value
SNMPv3 - v1v2only	subtree=1, included subtree=1.3.6.1.6.3.15, excluded subtree=1.3.6.1.6.3.16, excluded subtree=1.3.6.1.6.3.18, excluded
FTP - port	21 (not configurable)
Browser upgrade option	Enabled, (not configurable)
STP Fast	Disabled
HTTPS Port	Disabled

Physical and environmental specifications

Category	Specification
DC inputs	12 VDC: 4.0 A maximum per switch
Power consumption	50 W maximum per switch
Operating temperature	10° to 35° C (50° to 95° F)
Storage temperature	-40° to 70° C (-40° to 158° F)
Operating humidity	5% to 95% RH noncondensing
Storage humidity	5% to 95% RH noncondensing
Switch dimensions	267.7 x 192.79 x 27.94 mm (10.5 x 7.5 x 1.1 in.)
Weight	1.7 Kg (3.7 lbs.)
Safety	• TUV to UL 60950-1, and CAN/CSA C22.2 No. 60950-1 and to EN 60950-1 • CE Marking • RoHS 5/6 compliant

Performance specifications

Category	Specification
Transmission method	Cut through
Memory	256 MB main, 32 MB flash, and 1.5 MB shared packet buffer memory per switch
MAC address table size	8 KB per switch
Packet forwarding rate	1,488,095 packets per second with 64 byte packets per port (for 1000 Mb/s)
Maximum external port packet forwarding rate	5 X 1 Gb port = 5 X 1,488,095 = 7,440,475 pps per switch

Category	Specification
Best downlink external port packet forwarding rate ratio	16 : 5
Interswitch x-connects across enclosure backplane	1 X 10 Gb port
MAC address learning	Automatic update
Forwarding table age time	Maximum age: 1 to 1,000,000 seconds Default: 300 seconds

Performing a serial download

In this section

Introduction

Perform a serial download of the switch operating system firmware, or boot code firmware if upgrading a switch directly from any existing OS or boot code images.

This procedure requires:

- A computer running terminal emulation software
- A standard null modem cable with a female DB-9 connector
- A switch OS firmware and/or boot code images

Serial upgrade of boot code firmware image procedure

To perform a serial upgrade of the switch boot code firmware image, usually named `GbE2c-1-10G_b_100.bin`:

1. Using the null modem, connect the console port of the switch to the serial port of a PC that supports XModem/1K XModem.
2. Start HyperTerminal (part of Microsoft Windows) or equivalent terminal emulation application (depending on the computer operating system), and set the parameters for the terminal emulation console:

Parameter	**Value**
Baud rate	9600
Date bits	8
Parity	None
Stop bits	1
Flow control	None

3. Power on the switch.

4. Hold down the Shift key and press the D key repeatedly during the Memory Test, until this message appears:

```
Memory Test ..............................

Xmodem Mode

PPCBoot 0.0.0.11 (Count)


Memory Test (0x00) ..................................................... PASSED
Extended Memory Test (0x01) ............................................ SKIPPED
ECC Memory Test (0x01) ................................................. PASSED
I2C Test (0x02) ........................................................ PASSED
Flash Init (0x04) ...................................................... PASSED
Flash Protect Check (0x05) ............................................. PASSED
Flash Memory Test (0x06) ............................................... SKIPPED


Entering Fast (115200) Xmodem Mode ...


To download an image use 1K Xmodem at 115200 bps.

NOTE:  Once you change the baud rate, hit the <ENTER> key
       before initiating the download.

    ... Waiting for the <Enter> key to be hit before the download can start...



   .... Please initiate the transfer now ....
```

NOTE: To perform serial downloads at 57600 baud rate, press the Shift-F keys. To perform serial downloads at 115200 baud rate, press the Shift-D keys.

5. After the message in Step 4 appears, reconfigure the terminal emulation console using these parameters.

Parameter	Value
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

6. Press the Enter key several times on the PC that is connected to the console port of the switch. When the console port is successfully communicating with the PC, indicating readiness for image transfer, continuous C's appear:

```
CCCCCCCCCCCCCCCC
```

7. Be sure that the new switch boot code firmware file is available on the computer. This file can be downloaded from the CD that is shipped with the switch or from the HP website (http://www.hp.com/go/bladesystem/documentation).

8. Select **<Transfer-Send File>** from the menu and choose these options in the Send File window:

```
file: GbE2c-1-10G_b_100.bin (100 represents the version number of Switch Boot Code firmware)

protocol:  1K XMODEM
```

The Send File window displays progress of the file transfer. The file transfer might take up to seven minutes.

NOTE: Although slower, XModem also works if 1K MODEM is not used.

9. After completing the transfer, a message displays how many bytes transferred, followed by another message displaying the status of image extraction. Do not power cycle the switch during this process. After extracting the image, it is updated to flash and a message with a progress indicator displays as shown.

```
Total bytes transferred: 0x512400
```

△ **CAUTION:** Do not power off the switch until the message: "Change your baud rate to 9600 bps and power cycle the switch," is displayed, otherwise, the switch will be inoperable.

```
Verifying the CRC for RAM Disk Image ...  OK.
Writing RAM Disk Image to flash ...
*** DO NOT POWER OFF OR RESET THE SWITCH UNTIL COMPLETE ***
###################
The flash update is complete.


Verifying the CRC for Linux ...  OK.
Writing Linux to flash ...
*** DO NOT POWER OFF OR RESET THE SWITCH UNTIL COMPLETE ***
##
The flash update is complete.


Verifying the CRC for PPCBoot ...  OK.
Writing PPCBoot to flash ...
*** DO NOT POWER OFF OR RESET THE SWITCH UNTIL COMPLETE ***
#
The flash update is complete.


Change your baudrate to 9600 bps and power cycle the switch
```

10. Change the baud rate to 9600 and power off the switch, wait for a few seconds, and power on the switch.

The switch boots with the new version of the boot code image that was just downloaded.

Serial upgrade of operating system firmware procedure

To perform a serial upgrade of the switch operating system firmware image, usually named `GbE2c-1-10G_100.bin`:

1. Using the null modem cable, connect the console port of the switch to the serial port of a PC that supports XModem/1K XModem.
2. Start HyperTerminal (part of Microsoft Windows) or equivalent terminal emulation application (depending on the computer operating system) and set the parameters for terminal emulation console:

Parameter	Value
Baud rate	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

3. Power on the switch.
4. Hold down the Shift key and press the D key repeatedly during the Memory Test, until this message appears:

```
Memory Test ..............................

Xmodem Mode

PPCBoot 0.0.0.11 (Count)


Memory Test (0x00) ..................................................... PASSED
Extended Memory Test (0x01) ............................................ SKIPPED
ECC Memory Test (0x01) ................................................. PASSED
I2C Test (0x02) ........................................................ PASSED
Flash Init (0x04) ...................................................... PASSED
Flash Protect Check (0x05) ............................................. PASSED
Flash Memory Test (0x06) ............................................... SKIPPED


Entering Fast (115200) Xmodem Mode ...


To download an image use 1K Xmodem at 115200 bps.

NOTE:  Once you change the baud rate, hit the <ENTER> key
       before initiating the download.

    ... Waiting for the <Enter> key to be hit before the download can start...



   .... Please initiate the transfer now ....
```

NOTE: To perform serial downloads at 57600 baud rate, press the Shift-F keys. To perform serial downloads at 115200 baud rate, press the Shift-D keys.

5. After the message in Step 4 appears, reconfigure the terminal emulation console using these parameters.

Parameter	Value
Baud rate	115200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

6. Press the Enter key several times on the PC that is connected to the console port of the switch. When the console port is successfully communicating with the PC, indicating readiness for image transfer, continuous C's appear:

```
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

7. Be sure that the new switch operating system firmware file is available on the computer. This file can be downloaded from the CD that is shipped with the switch or from the HP website (http://www.hp.com/go/bladesystem/documentation).
8. Select **<Transfer-Send File>** from the menu and choose these options in the Send File window:

```
file: GbE2c-1-10G_100.bin (100 represents the version number of Switch WebOS firmware)

protocol:  1K XMODEM
```

The Send File window displays the progress of the file transfer. The file transfer might take up to five minutes.

NOTE: Although slower, XModem also works if 1K MODEM is not used.

9. After completing the transfer, a message displays how many bytes transferred, followed by another message displaying the status of image extraction. Do not power cycle the switch during this process.

```
Total bytes transferred: 0x33b400
```

△ **CAUTION:** Do not power off the switch until the message: "Change your baud rate to 9600 bps and power cycle the switch," is displayed, otherwise, the switch will be inoperable.

10. After extracting the image, the system prompts to select which current operating system image (image1 or image2) needs to be updated by the new operating system image. It also provides an option (n) not to update any and to quit the update procedure.

Depending on the selection, 1 or 2, the system updates image1 or image2 on the flash and a message with a progress indicator displays as shown below. If selecting n, the system aborts the update procedure and prompts to reset the baud rate and power cycle the switch.

```
Do you want this saved in Alteon OS Image Slot 1 or 2 (or A to abort)? 1

Verifying the CRC for WebOS Image ...  OK.
Writing WebOS Image to flash ...
*** DO NOT POWER OFF OR RESET THE SWITCH UNTIL COMPLETE ***
#############
The flash update is complete.

Change your baudrate to 9600 bps and power cycle the switch
```

11. Change the baud rate to 9600 and power off the switch. Wait for a few seconds, and power on the switch.

    During bootup the switch the following prompt appears:

```
Press <Ctrl>-o to use the other image…
```

    To use the other operating system image, press the Ctrl-o keys.

SNMP MIBs support

In this section

MIB overview

Management and statistics information is stored in the switch in the MIB. The switch supports several standard MIBs. Values for MIB objects are retrieved with any SNMP-based network management software.

In addition to the standard MIBs, the switch also supports its own proprietary enterprise MIB as an extended MIB. The proprietary MIB is retrieved by specifying the MIB OID at the network manager station.

MIB values are either read-only or read/write variables.

- Read-only MIB variables are constants that are programmed into the switch or variables that change while the switch is in operation. Examples of read-only constants include the number and types of ports. Examples of read-only variables are the statistics counters, such as the number of errors that have occurred or how many kilobytes of data have been received and forwarded through a port.
- Read/write MIB variables are usually related to user-customized configurations. Examples include the IP address of the switch, Spanning Tree Algorithm parameters, and port status.

SNMP Manager software

Using third-party vendor SNMP software to manage the switch allows access to proprietary enterprise MIBs for the switch. The MIBs are found in the utilities on the HP website (http://www.hp.com/go/bladesystem/documentation).

If the software provides functions to browse or modify MIBs, the MIB values (if the MIB attributes permit the write operation) are changeable. This process can be quite involved, because the MIB OIDs (available in the MIB files) must be used and retrieved one by one.

Use an SNMP manager, such as HP OpenView Network Node Manager or HP Systems Insight Manager, to access the enterprise-specific MIBs. Compile the MIBs into the MIB database and then use a MIB browser to navigate through them. For detailed information, access the individual descriptions of each MIB or see the documentation that came with the SNMP manager software.

The switch SNMP agent supports SNMP Version 1. Security is provided through SNMP community strings. The default community strings are "public" for SNMP GET operation and "private" for SNMP SET operation.

Users can specify up to two trap hosts for receiving SNMP traps. The agent sends the SNMP trap to the specified hosts when appropriate. Traps are not sent if there is no host specified.

Supported MIBs

The SNMP agent for the switch supports these MIBs:

- dot1x.mib
- GbE2c-1-10G-L2L3.mib
- GbE2c-1-10G-L2L3_cpqhost.mib
- GbE2c-1-10G-L2L3_cpqrack.mib
- GbE2c-1-10G-L2L3_cpqsinfo.mib
- rfc1213.mib
- rfc1215.mib
- rfc1493.mib
- rfc1573.mib
- rfc1643.mib
- rfc1757.mib
- rfc1907.mib
- rfc2037.mib
- rfc2571.mib
- rfc2572.mib
- rfc2573.mib
- rfc2574.mib
- rfc2575.mib
- rfc2576.mib

Supported traps

The switch SNMP agent supports these traps:

- rfc1215.mib traps
  - coldStart
  - warmStart
  - linkDown
  - linkUp
  - authenticationFailure
  - egpNeighborLoss
- rfc1493.mib traps
  - newRoot
  - topologyChange
- rfc1757.mib traps

- risingAlarm
- fallingAlarm

- GbE2c-1-10G-L2L3.mib traps
  - bntSwDefGwUp
  - bntSwDefGwDown
  - bntSwDefGwInService
  - bntSwDefGwNotInService
  - bntSwLoginFailure
  - bntSwTempExceedThreshold
  - bntSwApplyComplete
  - bntSwSaveComplete
  - bntSwFwDownloadSucess
  - bntSwFwDownloadFailure
  - bntSwTempReturnThreshold
  - bntSwUfdfoLtMFailure
  - bntSwUfdfoLtMUP
  - bntSwUfdfoGlobalEna
  - bntSwUfdfoGlobalDis
  - bntSwUfdfoLtDAutoEna
  - bntSwUfdfoLtDAutoDis
  - bntSwStgNewRoot
  - bntSwCistNewRoot
  - bntSwStgTopologyChanged
  - bntSwCistTopologyChanged
  - bntSFPInserted
  - bntSFPRemoved

Electrostatic discharge

In this section

Preventing electrostatic discharge

To prevent damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding methods to prevent electrostatic discharge

Several methods are used for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm ±10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part.

For more information on static electricity or assistance with product installation, contact an authorized reseller.

RJ-45 pin specification

In this section

Standard RJ-45 receptacle/connector

When connecting the switch to a switch, bridge, or hub, an Ethernet cable is necessary.

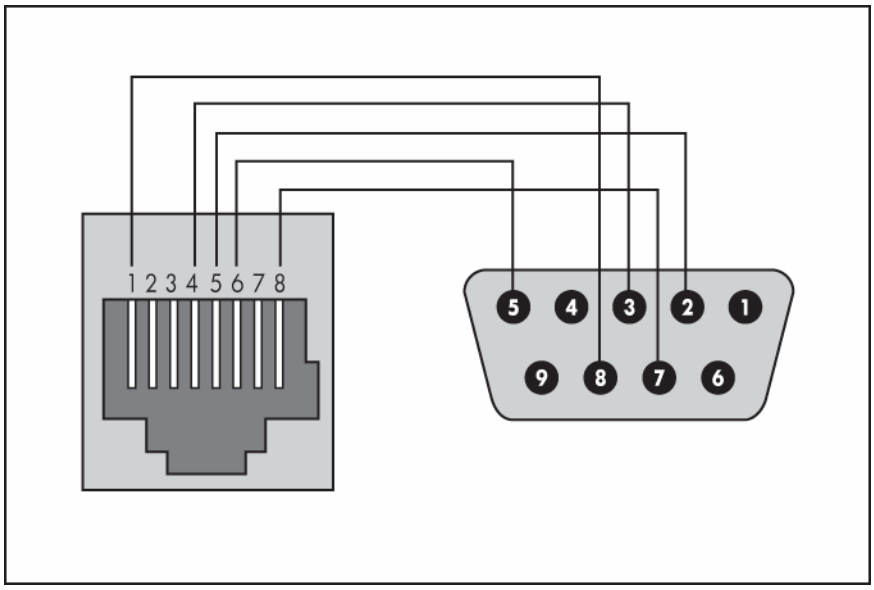
The table indicates the pin number and wire color assignments for the switch-to-network adapter card connection, and the Ethernet cable for the switch-to-switch, switch-to-hub, or switch-to-bridge connection.

Contact	Media direct interface signal	Color match
1	Tx + (transmit)	White/Orange
2	Tx - (transmit)	Orange/White
3	Rx + (receive)	White/Green
4	Not used	Blue/White
5	Not used	White/Blue
6	Rx - (receive)	Green/White
7	Not used	White/Brown
8	Not used	Brown/White

The table provides the same information for the Gigabit over Copper ports.

Contact	Media direct interface signal	Color match
1	BI_DA+	White/Orange
2	BI_DA-	Orange/White
3	BI_DB+	White/Green
4	BI_DC+	Blue/White
5	BI_DC-	White/Blue
6	BI_DB-	Green/White
7	BI_DD+	White/Brown
8	BI_DD-	Brown/White

RJ-45 to DB-9 serial adapter with flow control pin assignment



RJ-45 signals	RJ-45 pins	DB-9 pins	DB-9 signals
Request to send (RTS)	1	8	Clear to send (CTS)
Data set ready (DSR)	2		
Data carrier detect (DCD)	3		
Receive data (RxD)	4	3	Transmit data (TxD)
Transmit data (TxD)	5	2	Receive data (RxD)
Ground (GND)	6	5	Ground (GND)
Data terminal ready (DTR)	7		
Clear to send (CTS)	8	7	Request to send (RTS)
(Not connected)	9		

Troubleshooting

In this section

Forgotten administrator user name and password that was configured on the switch

Action:

Call HP technical support at 1-800-652-6672, or call a service representative to get a backdoor password.

Health LED on the switch is not on

Action:

- The switch is not seated properly. Be sure that the switch is inserted completely and seated properly.

- The server blade enclosure is not powered up. Be sure that the server blade enclosure is powered up and all the power connections are intact.
- There is a faulty LED. Check the console to see if the switch is booted.
- The switch fuse is blown. Send for repair.

Health LED on the switch stays amber for more than 30 seconds and switch does not boot

Action:

The Standby Mode Timeout function is malfunctioning. Force the switch to reboot by pressing the **Reset** button.

No link LED appears, even after plugging the Category 5 cable in the RJ-45 connector of the external port

Action:

- The cable is not properly plugged in. Check the cable at both ends to ensure that it is plugged in and seated properly.
- The cable or connector heads are faulty. Replace the cable with another tested cable.
- The RJ-45 connector on the switch or LED is faulty.
  - After checking and replacing the cable, if no link LED displays, check whether the port is transferring data. If yes, the LED is faulty. If no, it could be a faulty RJ-45 connector. Call a service representative.
  - This could be caused by using a crossover cable instead of a straight through cable.

Cannot access the switch serial console interface using null modem connection from a PC Terminal Emulation Program

Action:

- The null modem cable is faulty. Be sure the null modem cable, provided by HP with this hardware, was used.
- The connection settings do not match the switch serial settings. Be sure that the PC Terminal Emulation session settings match the switch serial settings.

Error message that the switch failed to complete the system self-testing appears on the serial console screen

Action:

The system diagnostic tests failed. Note the reason for the failure from the serial console screen message and call a service representative.

The switch fails to get its IP settings from the BOOTP server, even though by default it is configured for BOOTP

Action:

- The switch is not connected properly to the network. Check the cable and connections and be sure that there is network connectivity between the switch and the BOOTP server.
- The BOOTP server is not available on the network or VLAN that is attached to the switch management port. Be sure that the BOOTP server is present on the network or VLAN attached to the switch.
- The BOOTP server cannot offer IP settings to the switch because no IP addresses are available. Add additional IP addresses as necessary.
- The switch timed out its request for IP settings. Reset the switch.

The keyboard locks up when using HyperTerminal to log on to the switch through the console interface

Action:

Scroll lock is on. Press the Scroll Lock key on the keyboard and be sure that the scroll lock is off.

Cannot connect to the switch console interface remotely using Telnet

Action:

- The switch IP address is not configured or correct.
  - From the serial console interface, be sure that the switch IP address is configured and valid on the network.
  - Use the correct IP address to establish the Telnet connection with the switch.

- The setting allowing access to the switch using the Telnet interface is disabled. From the serial console interface, be sure that the Telnet interface is enabled.
- The management network address/mask (if used) does not contain the IP address of the management station. From the serial console interface, be sure that the Management Network Address/Mask contains the IP address of the management station.

Password is not accepted by the switch using the remote console interface immediately after a reboot

Action:

The switch is still working on network convergence. Wait up to 10 seconds for the password to be accepted.

Cannot connect to the switch console interface remotely using SSH

Action:

- The switch IP address is not configured or correct.
  - From the serial console interface, be sure that the switch IP address is configured and valid on the network.
  - Use the correct IP address to establish the SSH connection with the switch.
- The setting allowing access to the switch using the SSH interface is disabled.
- From the serial console interface, be sure that the SSH interface is enabled and all the settings are configured correctly.
- The management network address/mask (if used) does not contain the IP address of the management station. From the serial console interface, be sure that the management network address/mask contains the IP address of the management station.

Cannot connect to the switch SNMP interface

Action:

- The switch IP address is not configured or correct.
  - From the serial console interface, be sure that the switch IP address is configured and valid on the network.
  - Use the correct IP address to establish the SNMP connection with the switch.
- The management network address/mask (if used) does not contain the IP address of the management station. From the serial console interface, be sure that the management network address/mask contains the IP address of the management station.

The port activity LEDs continuously indicate activity after connecting more than one port to another switch or destination device

Action:

Because there are multiple links across this device and the destination device, they form loops, which cause broadcast storms. Enable STP for multiple links. This setting prevents loops and maintains standby links for resilience in case of primary link failure.

Cannot connect to the switch remotely using the Web interface

Action:

- The switch IP address is not configured or correct.
  - From the serial console interface, be sure that the switch IP address is configured and valid on the network.
  - Use the correct IP address to establish the Web connection with the switch.
- Access to the switch using the Web interface is disabled. From the serial console interface, be sure that the Web interface is enabled.
- The Proxy server settings are configured on the Internet browser and the proxy server does not know the switch IP address. Disable the manual proxy settings on the Web browser and let it automatically find Web servers using the IP address.
- The management network address/mask (if used) does not contain the IP address of the management station. From the serial console interface, be sure that the management network address/mask contains the IP address of the management station.

Cannot enable a port in multiple VLANs while configuring VLANS

Action:

A port is part of only one VLAN unless the port is a tagged port. Be sure that the port is enabled as a tagged port.

The switch does not let the user enable two adjacent ports into two different VLANs while assigning the ports to VLANs

Action:

The ports are two adjacent ports that are bundled in a Port Trunk. Two ports that are assigned to a Port Trunk cannot be assigned to two different VLANs. Either break the trunk to assign it two different VLANs or assign the ports to one VLAN.

While using TFTP to download firmware, the switch fails to connect to the TFTP server, or after connection the download fails

Action:

- The TFTP server is not available to connect to or there is connectivity failure between the switch and TFTP server.
  - Be sure that the IP address of the TFTP server is correct.
  - Be sure that the TFTP server exists on the same network and VLAN as the switch.
  - Be sure that the TFTP server can be pinged from the switch and vice versa.
- The firmware file is not found on the TFTP server. The file name could be wrong.
  - Be sure that a valid firmware file exists on the TFTP server to download to the switch.
  - On the switch, check the file name configured to download.
- The TFTP server was started with a configured directory. The switch must be configured using the full path name, if it is not in the directory specified in the TFTP server.

The switch fails to connect to the TFTP server while using TFTP to download or upload a configuration file, or after connection the download or upload fails

Action:

- The TFTP server is not available to connect or there is a connectivity failure between the switch and the TFTP server.
  - Be sure that the TFTP server exists on the same network or VLAN as that of the switch.
  - Be sure that the TFTP server can be pinged from the switch and vice versa.
  - Be sure that the IP address of the TFTP server is correct.
- The configuration file is not found on the TFTP server. The file name could be wrong.

- Be sure that a valid configuration file exists on the TFTP server to download to the switch.
- On the switch, check the file name configured to download or upload.

- The TFTP server was started with a configured directory. The switch must be configured using the full path name, if it is not in the directory specified in the TFTP server.

The console screen displays a message to change the baud rate for the terminal emulation session for XModem transfer after forcing the switch into the download mode, and does not display CCCC...

Action:

The terminal emulation session baud rate does not match the switch serial console baud rate in the download mode. Change the baud rate of the terminal emulation session to match the switch serial console baud rate in the download mode.

IMPORTANT: The baud rate for the switch serial console in the download mode and runtime mode are two separate settings.

The download fails after starting to download the firmware file

Action:

The firmware file is not the correct one or is corrupt. Obtain the latest firmware file that is specified for this switch.

The switch configuration is corrupt

Action:

An error was made when saving the switch configuration. Reboot the switch and reload the factory settings. This action clears all settings and restores them to the initial values that were present when the switch was purchased. See the *HP GbE2c Ethernet Blade Switch for c-Class BladeSystem Command Reference Guide* for more information.

After reloading the factory settings, reconfigure the switch settings.

XFP transceiver port is disabled

Action:

Verify the XFP transceiver was purchased from HP. To purchase an XFP transceiver from HP, contact an authorized HP reseller.

Acronyms and abbreviations

AAA

authentication, authorization, and accounting

BBI

browser-based interface

BOOTP

Bootstrap Protocol

CLI

Command Line Interface

CPU

central processing unit

CSMA/CD

Carrier Sense Multiple Access with Collision Detection

DNS

domain name system

FDB

forwarding database

FTP

file transfer protocol

GMT

Greenwich mean time

HTTP

hypertext transfer protocol

HTTPS

hypertext transfer protocol secure sockets

IEEE

Institute of Electrical and Electronics Engineers

IGMP

Internet Group Management Protocol

IP

Internet Protocol

iSCLI

industry standard command line interface

LACP

Link Aggregation Control Protocol

LAN

local-area network

MAC

medium access control

MAU

media attachment unit

MDI

medium dependent interface

MDI-X

medium dependent interface-crossover

MIB

management information base

MSTP

Multiple Spanning Tree Protocol

NAS

network access server

NIC

network interface controller

NTP

network time protocol

NVRAM

non-volatile memory

OID

object identifier

OS

operating system

OSI

Open Systems Interconnection

OSPF

open shortest path first

POST

Power-On Self Test

PXE

Preboot Execution Environment

RADIUS

Remote Authentication Dial-In User Service

RAS

remote access service

RFC

request for comments

RIP

routing information protocol

RMON

remote monitoring

RSTP

Rapid Spanning Tree Protocol

SCP

Secure Copy

SFP

small form-factor pluggable

SNMP

Simple Network Management Protocol

SSH

Secure Shell

STP

Spanning Tree Protocol

TACACS+

Terminal Access Controller Access Control System Plus

TFTP

Trivial File Transfer Protocol

UDP

User Datagram Protocol

UFD

uplink failure detection

UTP

unshielded twisted pair

VID

VLAN ID

VLAN

virtual local-area network

VRRP

virtual redundant router protocol

XFP

10 Gb small form factor pluggable

Index

R

S

T

U

V

X